CLAIMS

1. A method for providing cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the method executable by a first computer node comprising the steps of:

- generating a random secret key;

- generating an exponent interval having a first random limit, wherein, with a probability close to certainty, each element of the exponent interval has a unique prime factor that is larger than a given security parameter;

- providing a public key comprising an exponent-interval description and a public key value derived from the random secret key, such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

2. The method according to claim 1, wherein the step of generating a random secret key comprises using two primes, the product of which is part of the public key.

3. The method according to claim 1, wherein the step of generating a random secret key comprises selecting an integer value defining a class group and selecting two elements of the class group.

4. The method according to claim 3, wherein the step of providing a public key comprises computing a modified public key value under use of the selected two elements and the exponent interval.

5. A method for providing a signature value on a message in a network of connected computer nodes, the method executable by a first computer node comprising the steps of:

- selecting an exponent value from an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and

- deriving the signature value from a provided secret key, the selected exponent value, and the message, the signature value being sendable within the network to a second computer node for verification.

6. The method according to claim 5, wherein the step of deriving the signature value further comprises a computation of the *i*-th root of a value derived from the message and the secret key using a cryptographic hash function, the *i* being the exponent value.

7. A method for verifying a signature value on a message in a network of connected computer nodes, the method executable by a second computer node comprising the steps of:

- receiving the signature value from a first computer node; and
- verifying whether an exponent value is contained in an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter , the signature value is invalid if the exponent value is not contained in the exponent interval.

8. The method according to claim 7, wherein the step of verifying further comprises a computing step of raising a computed signature root value that being part of the signature value to the power of the exponent value.

9. An apparatus to provide a signature value on a message in a network of connected computer nodes, the apparatus executable by a first computer node comprising:

- means for selecting an exponent value from an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and

- means for deriving the signature value from a provided secret key, the selected exponent value, and the message, the signature value being sendable within the network to a second computer node for verification.

10. An apparatus to verify a signature value on a message in a network of connected computer nodes, the apparatus executable by a second computer node comprising:

- means for receiving the signature value from a first computer node; and

- means for verifying whether an exponent value is contained in an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter , the signature value is invalid if the exponent value is not contained in the exponent interval.

11. A computer device comprising:

a computer program product according to claim 9; and

a processor for executing the computer program product when the computer program product is run on the computer device.

12. An apparatus to provide cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the apparatus executable by a first computer node comprising:

- means for generating a random secret key;

- means for generating an exponent interval having a first random limit, wherein, with a probability close to certainty, each element of the exponent interval has a unique prime factor that is larger than a given security parameter; and

- means for providing a public key comprising an exponent-interval description and a public key value derived from the random secret key, such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

13. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing provision of cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

14. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing

cryptographic keys usable in a network of connected computer nodes applying a signature scheme, said method steps comprising the steps of claim 1.

15. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing provision of a signature value on a message in a network of connected computer nodes, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 5.

16. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing a signature value on a message in a network of connected computer nodes, said method steps comprising the steps of claim 5.

17. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing provision of a signature value on a message in a network of connected computer nodes, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 7.

18. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing a signature value on a message in a network of connected computer nodes, said method steps comprising the steps of claim 7.

19. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing provision of a signature value on a message in a network of connected computer nodes, the computer

readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 9.

20. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing verification of a signature value on a message in a network of connected computer nodes, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 10.

21. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing provision of cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 12.